Digital Medicine, Cybersecurity, and Ethics: An Uneasy Relationship

Weber, Karsten ; Loi, Michele ; Christen, Markus ; Kleine, Nadine

Abstract: Comment on The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine. [Am J Bioeth. 2018]

DOI: https://doi.org/10.1080/15265161.2018.1498935

Digital medicine, cybersecurity and ethics: An uneasy relationship

Journal:	*American Journal of Bioethics*
Manuscript ID	UAJB-2018-0276.R1
Manuscript Type:	Open Peer Commentary

Digital medicine, cybersecurity and ethics: An uneasy relationship

The paper of Klugman et al. has the merit of pointing out in great detail, which ethical questions will be raised if in the near future sophisticated mobile (and partly implantable) information technology devices are used in healthcare to monitor patients and to provide targeted therapeutic interventions such as drug applications or neuronal stimulation. Such "self-acting medical devices" (in the following we use the acronym SAMD; "smart pills" are one type of a SAMD application) will require sophisticated information technology including sensor, computation, communication and actor (e.g. drug release systems) capabilities in order to function properly. In our contribution, we complement the "ethical landscape" of Klugman et al. by adding an important, but often neglected dimension: the *cybersecurity* of such systems and the ethical issues raised by enforcing it. Our considerations are based on the findings of the ongoing, EU-funded project CANVAS (https://canvas-project.eu/canvas/) on the ethics of cybersecurity.

Following the *International Telecommunication Union* definition, cybersecurity involves the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets". Cybersecurity thus involves a broad spectrum of desiderata that sophisticated information and communication technology (ICT) systems such as SAMDs should comply to. Those include:

- *Quality and efficiency of services:* One of the main purposes of ICT systems in healthcare is the administration of information about patients and treatments in order to increase efficiency and to reduce costs. Quality, as distinct from efficiency, refers to improvements in healthcare of qualitative, not only quantitative nature.
- *Privacy of information and confidentiality of communication:* Privacy and confidentiality are important desiderata of services in the medical domain. The notion of privacy concerns information that is not meant to be shared with anyone, while confidentiality implies the protection of communication channels between a SAMD and trusted parties. This may require the use of technological means such as encryption that are energy costly.
- *Usability:* ICT is designed to afford usability, i.e., "the degree of effectiveness, efficiency, and satisfaction with which users of a system can realize their intended task" (Roman et al., 2017, p. 70). Depending on the function of the ICT system in question, users can be patients, health workers and professionals, administrators, or a combination of these.
- *Safety:* Safety can be defined as the reduction of health-threatening risks and risks to persons' health. Safety can be distinguished from quality, in that, for example, a SAMD can both enable therapies of higher quality and simultaneously expose patients to new risks, e.g. in the event of a cyberattack.

Those desiderata obviously also relate to SAMDs; and several of the considerations of Klugman et al. actually concern ethical implications of those desiderata (e.g., regarding the confidentiality of data or trusting the device). However, enforcing cybersecurity of SAMDs through means such as encrypted communication, security protocols on the level of clinicians that supervise a SAMD or data management training do involve additional ethical issues. As the principles of biomedical ethics originally introduced by Beauchamp and Childress (1979) are a well-known ethical framework within bioethics, we use it here to outline briefly some value conflicts that may emerge when SAMDs should comply with the desiderata mentioned above:

Beneficence and autonomy vs. non-maleficence and justice: Suppose that cybersecurity in healthcare should optimize quality and efficiency of healthcare services as well as privacy of information and confidentiality of communication. Such a design could be responsive to the

individual preferences of patients, while protecting their privacy (which relates to the principle of autonomy mentioned by Beauchamp and Childress) and allocating resources efficiently (which relates to the principle of beneficence). But a SAMD capable of achieving this will tend to be quite complex and, as such, compromises usability. For example, it may prevent certain patient groups from using such a device, which would be a conflict with the justice principle. SAMDs with extended networking capabilities and privacy protections may also reduce usability in critical situations (for instance with regard to complex authorization procedures) and thus affects safety, which is in tension with the principle of non-maleficence. Finally, such design choices may conflict with justice in relation to privacy and safety: A platform for accessing SAMD data with complex authentication (e.g. long and difficult passwords) may encourage workarounds (e.g. writing passwords in unsafe places) in particular among less tech-savvy users.

Beneficence and autonomy vs. non-maleficence and autonomy: Consider highly networked, data-intensive SAMDs designed to benefit people with better and more cost-effective healthcare services while respecting their autonomy. If the system involves complex, granular, stratified authorization systems requiring complex passwords, it again may invite workarounds, which undermines cybersecurity. This generates exposure to passive and active attackers, who may interfere with a device or gain access to confidential information, which is in conflict with both the principles of non-maleficence and (privacy-related) autonomy.

Beneficence, justice and non-maleficence vs. autonomy and non-maleficence: Suppose, for instance, SAMDs making extensive use of patients' surveillance with good protection of data integrity and accessibility but poor protection for confidentiality and privacy. Again, a design of this kind may comply with some aspects of the principle of beneficence and some aspects of non-maleficence, but would sacrifice autonomy due to patient surveillance and privacy violations as well as other aspects of non-maleficence. Incidentally, such design may be compatible with justice only because it 'levels down' privacy and autonomy for all patients.

Non-maleficence and autonomy vs. beneficence and autonomy: Consider SAMDs optimized to promote privacy and safety. An extreme form of this would be SAMDs minimizing data collection, data sharing, communication and networking; i.e. the system would have advanced autonomous capabilities in order to be able to deal with unexpected situations. Such system may actually be able to avoid privacy breaches and device malfunctions. It would thus be responsive to the principle of non-maleficence and autonomy, as far as it protects privacy, which is crucial for autonomy. However, such SAMDs could not be used for providing data-intensive services, which may involve a sacrifice in quality and/or cost-effectiveness contrary to the principle of beneficence. Furthermore, the energy needs of such advanced autonomous technology are likely to be high, which again would impede some aspects of usability with implications on autonomy and beneficence.

Justice vs. autonomy and non-maleficence: A design choice may promote quality and efficiency while equalizing safety and privacy for different demographics. Think about a SAMD with a relatively simple authentication system and few or merely one-size-fit-all privacy options. Complex authentication systems would then be avoided. It may be more suitable for patients from certain demographics (e.g. elderly or people lacking digital literacy) who may actually gain autonomy, paradoxically, thanks to a system that offers few personalization options and is therefore simple to use. Less sophisticated ICT users would also be less tempted to find workarounds to security, so these SAMDs may achieve a more even level of security. Their design might reach a more equal distribution of benefits as it would be easier for otherwise disadvantaged users to take advantage of it. Such SAMDs would be compatible with justice but would be incompatible with services that are very complex except in ways that imply extensive patient surveillance across all spheres of human life. It would also conflict with the principle of non-maleficence in that it would feature weak authentication, which could put the privacy of the most vulnerable individuals at risk.

This brief analysis outlines that trade-offs involved in design choices concerning cybersecurity for SAMDs map onto conflicts among the four principles of bioethics. These trade-offs and the corresponding conflicts seem unavoidable. As Beauchamp and Childress' principlism does not provide priority rules for balancing the four principles when they conflict, balancing them is left to the wisdom of ethical decision makers (e.g. physicians, ICT developers and administrators). As a prerequisite, this requires awareness of such conflicts and – in a next step and using the words of Klugman et al. – "planning for, and iteratively addressing the array of ethical issues". For doing this, it would be wise to expand the spectrum of ethical investigation on the cybersecurity implications of SAMDs.

References

Beauchamp, Tom L., and James F. Childress. 1979. Principles of biomedical ethics. New York: Oxford University Press.

ITU. 2008. International Telecommunications Union, ITU-TX.1205: Series X: Data networks, open system communications and security: Telecommunication security: Overview of cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I.

Roman, Lisette C., Jessica S. Ancker, Stephen B. Johnson, and Yalini Senathirajah. 2017. "Navigation in the electronic health record: A review of the safety and usability literature". Journal of Biomedical Informatics 67 (3): 69–79. https://doi.org/10.1016/j.jbi.2017.01.005.